DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Name of MACOM/DA Staff Proponent (APMS Sub Organization Name)

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (F&MWRC)

2. Name of Information Technology (IT) System (APMS System Name)

Army Volunteer Management System (AVMS)

3. Budget System Identification Number (SNAP-IT Initiative Number)

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR))

594

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable)

N/A

6. Privacy Act System of Records Notice Identifier (if applicable)

A0215-3 SAMR, NAF Personnel Records (June 1, 2000, 65 FR 35054);
OPM/GOVT-5, Recruiting, Examining, and Placement Records (June 19, 2006, 71 FR 35351)

7. OMB Information Collection Requirement Number (if applicable) and expiration date

N/A

8. Type of authority to collect information (statutory or otherwise)

5 U.S.C. 301, 1302, 3109, 3111, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533;
10 U.S.C. 1588 and 3013
26 U.S.C. 6041
Executive Order 9397 and 12072
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR)
DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR)

Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities
Army Regulation 608-1, ACS Policy & Family and Soldier Readiness System
Army Regulation 215-3, Non-appropriated Fund Personnel Policy
Army Regulation 215-4, Non-appropriated Fund Contracting
Army Regulation, 608-10 Child Development Services

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup)

The Army Volunteer Management Information System (AVMS) is an online system developed as a part of the directorate's portal to assist in the recruitment and management of volunteers. AVMS capabilities include: a) recruitment of volunteers throughout the Army by organization, military community, position; b) standardized position descriptions developed by headquarters, reducing installation work load and providing tracking of positions across the Army; c) individualized position descriptions developed by installations for unique jobs or responsibilities; d) easy and efficient communication among organizations, Army Volunteer Corps Coordinators, and volunteers; e) collection and certification of volunteer hours with real-time roll up to headquarters; f) volunteer service record maintained on line, to include positions, awards and training; g) storage of certificates of training, awards, credentials and background checks; identification of volunteers having background checks and the point of contact who conducted the check; h) rosters of volunteers and managers, with email and telephone numbers.

The system currently is deployed and is in the sustainment part of its lifecycle. FMWRC Family Programs Directorate owns the system. The system is comprised of an application server, database server, web server and file server. All servers communicate with the others through isolated and controlled Windows domain accounts. The system is located at DefenseWeb's collocation. Also, all servers have redundant fail over servers that are continually updated with content changes. All systems are backed up on a nightly and weekly schedule.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD)

The personally identifiable information (PII) collected into the system consists of the following elements: name, permanent and current addresses, phone numbers, date of birth, last four digits of Social Security Number, veterans' preference, spouse preference, citizenship e-mail address, employment history, relevant volunteer experience, education, pay, awards, training, references, previous supervisors' names, spouse names, security clearance levels, certificates, licenses, hobbies and interests. The sources are the Army Community Service (ACS) staff and the individual record subject.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection

Information will be entered by the ACS volunteers themselves and/or by ACS staff during personal interview. Volunteer opportunities are entered into the system by ACS staff.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program)

PII is collected to determine the qualifications of individuals to serve as volunteers; to establish and track an individual's volunteer service record; to assess volunteer trends and patterns; to determine historical, current and future needs; and to produce statistical studies and reports required by Assistant Secretary of Defense for Force Management and Personnel.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data)

PII will be used to recruit for volunteer opportunities online and to establish and track an individual's volunteer service record. Data is also used to assess staff and volunteer trends and patterns, to determine historical, current and future needs as well as to produce statistical studies and reports required by Assistant Secretary of Defense for Force Management and Personnel.

14. Describe whether the system derives or creates new data about individuals through aggregation

The system does not create new data through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies)

Developers, system administrators, ACS managers, staff members and volunteers will have access to some data in the system on a need to know basis. Reports are developed to answer HQDA taskers and DoD inquiries. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific

uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent

Before a client's record is entered into the system, a Privacy Act Statement is displayed giving a section on authority, principal purpose, routine uses, and disclosure for the system. The Privacy Act is read by the ACS Staff member to the client. No client information can be recorded until a checkbox has been checked by the Staff member acknowledging that they have spoken with the client about the Privacy Act information. Individuals can object or consent verbally at anytime during the data input process.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic), regarding the determination to collect the information in identifiable form

Before a client's record is entered into the system, a Privacy Act Statement is displayed giving a section on authority, principal purpose, routine uses, and disclosure for the system. The Privacy Act is to be read by the ACS Staff member to the client. No client information can be recorded until a checkbox has been checked by the Staff member acknowledging that they have spoken with the client about the privacy act information. Individuals can object or consent verbally at anytime during the data input process.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form

All ACS volunteers accessing government computer information are required to undergo and receive, at a minimum, a favorable local, state and national security checks in order to perform official government duties; they are limited to specific or general information in the computing environment; therefore, certain types of data are restricted to only certain access levels within the system. Each user has a unique username and password for the system.

All volunteers must register in the system to enter volunteer hours, review reports, or enter position vacancies. Each registered user is assigned an access level based upon his/her position. Training and user guides are developed to orient staff and advise of their authority levels and functionality within the system. The system tracks and calculates volunteer hours contributed and exports that data to the DA Form 4162, Volunteer Service Record, and the DA Form 4713, Volunteer Daily Time Record. Although this data could be found in paper form, the system allows managers to certify the volunteer hours that the paper forms do not.

Components of the system are set up to be accessed by levels. Certain types of data are restricted to specific access levels within the system. These access levels are assigned by system administrators to authorized personnel as needed. Data search results in the system are for one record only, as opposed to searching through multiple

data records. All data is filtered by installation and can not be searched by users not authorized for the particular installation for which the data is stored.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur

The System of Record Notice currently exists and will be updated to contain more specific information.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal; no risk when providing individuals an opportunity to object/consent.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form

The Privacy Act data in this system is For Official Use Only (FOUO); the PIA may be published in full.